

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

BLUE SPIKE, LLC

Plaintiff,

V.

VERIMATRIX,

Defendant.

§

2:16-cv-00329-RWS
LEAD CASE

JURY TRIAL DEMANDED

BLUE SPIKE, LLC

Plaintiff,

V.

MEDIA SCIENCE INCORPORATED,

Defendant.

2:16-cv-0701-RWS
MEMBER CASE

JURY TRIAL DEMANDED

**ADDITIONAL DOCUMENT RELATED TO DOCKET NO. 145-7 (DECLARATION OF
YANNIS PAKONSTANTINOU, PHD, IN SUPPORT OF BLUE SPIKE LLC'S CLAIM
CONSTRUCTION)**

Attached to this additional document cover page is EXHIBIT A to the declaration of Yannis Papakonstantinou filed at Dkt. No. 145-7 in support of Blue Spike's Opening Claim Construction Brief that the disputed patent terms/phrases are not indefinite.

Respectfully submitted,

/s/ Randall T. Garteiser

Randall T. Garteiser

Lead Attorney

Texas Bar No. 24038912

rgarteiser@ghiplaw.com

Christopher A. Honea

Texas Bar No. 24059967

chonea@ghiplaw.com

Kirk J. Anderson
California Bar No. 289043
kanderson@ghiplaw.com
Ian N. Ramage
California Bar No. 224881
iramage@ghiplaw.com
GARTEISER HONEA, P.C.
119 W Ferguson St
Tyler, Texas 75702
(888) 908-4400 phone/fax

Counsel for Blue Spike, LLC

Certificate of Service

The undersigned certifies that the foregoing document was filed electronically in compliance with Local Rule CV-5(a). As such, this document was served on all counsel deemed to have consented to electronic service. Local Rule CV-5(a)(3)(A). Pursuant to Federal Rule of Civil Procedure 5(d) and Local Rule CV-5(d) and (e), all other counsel of record not deemed to have consented to electronic service were served with a true and correct copy of the foregoing by email, on this date stamped above.

/s/ Randall Garteiser
Randall Garteiser

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

BLUE SPIKE, LLC

Plaintiff,

V.

VERIMATRIX,

Defendant.

[illegible]

2:16-cv-00329-RWS
LEAD CASE

JURY TRIAL DEMANDED

BLUE SPIKE, LLC

Plaintiff,

V.

MEDIA SCIENCE INCORPORATED,

Defendant.

2:16-cv-0701-RWS
MEMBER CASE

JURY TRIAL DEMANDED

**DECLARATION OF YANNIS PAPAKONSTANTINOU, PHD IN SUPPORT OF
BLUE SPIKE, LLC'S CLAIM CONSTRUCTION**

1. I, Yannis Papakonstantinou, do hereby state and declare the following:
 2. I write this declaration in support of Blue Spike's claim construction positions.
- It is my understanding that Media Science Incorporated ("MSI") alleges certain terms of the patents asserted in this case are indefinite. As one of ordinary skill in the art, it is my belief that none of the claims implicated by MSI is indefinite.
3. I am being paid for my work in this litigation at the rate of \$460 per hour. My compensation does not depend on the outcome of this litigation. I have no personal interest in the outcome.
 4. I hold a Diploma of Electrical and Computer Engineering from National Technical University of Athens (1990), as well as an M.S (1994) and Ph.D (1997) in

Computer Science from Stanford University. I have served as Program Chair and Program Committee Member of numerous conferences, member and chair of several USCD University committees, and am the recipient of several awards and fellowships.

5. I am currently a professor of Computer Science and Engineering at USCD University.

6. Attached hereto as Exhibit A is a true and correct copy of my curriculum vitae (“CV”). My CV includes a listing of publications I have authored.

7. In preparation for writing this declaration in support of Blue Spike’s claim construction positions and against MSI’s constructions of certain terms as indefinite, I have reviewed and opined on the Joint Claim Construction of Blue Spike and MSI and examined U.S. Patents Nos. 5,889,868 (the ’868 Patent), 7,877,609 (the ’609 Patent), and 8,307,213 (the ’213 Patent). I have also reviewed portions of U.S. Patents 7,362,775, 7,830,915, 7,770,017 and 8,774,216.

8. This declaration is based on my education, professional career and relevant experiences, as well as the materials reviewed. All of the opinions stated in this declaration are based on my own personal knowledge and professional judgment; if called as a witness in this matter, I am prepared to testify competently about them.

9. I am not a lawyer but have been informed on “definiteness” requirements of patent claims under Patent Law. The specific requirement I have been asked to address in this declaration is found in 35 U.S.C. § 112, Paragraph 2, which provides:

“The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.”

10. Applying the definiteness rule described above, I provide the remarks and analysis below, as viewed by a person of ordinary skill in the art at the time of the invention, regarding terms in the patents-in-suit which MSI believes to be indefinite:

11. '868 Patent, Claim 9, "the water mark message"

- a. A watermark message is readily understood by one of ordinary skill in the art as the watermark information encoded within a digital signal. In other words, a digital signal is watermarked with a watermark message. The term "watermark" and "watermark message" are often used interchangeably.
- b. And the term "watermark message" finds ample support in the specification of the '868 Patent. For instance, the patent teaches in Col. 3, ll. 10-17:

The present invention also relates to a method of amplitude independent decoding of digital watermark information in a signal including steps of determining in the signal a sample window having a minimum and a maximum, determining a quantization interval of the sample window, normalizing the sample window to provide samples, and **analyzing the quantization level of the samples to determine a message bit value.**

This passage describes how a watermark message is decoded from the digital signal.

Furthermore, The specification describes how a "watermark location is determined . . . on the creation of a pseudo-random key." '868 Patent, Col. 7, ll. 29-31. Three concepts are described here: the watermark message (here referred to as a "watermark"), the key, and the location to

place the watermark. Shortly thereafter, the specification explains how “an engineer seeking to provide high levels of protection of copyrights, ownership, etc. is concerned with the size of a given key, the size of the watermark message and the most suitable area and method of insertion.” ’868 Patent, Col. 7, ll. 35-39. Here we see the same three concepts as in the earlier portion of the specification, only “watermark message” is used instead of “watermark.” *See also*, ’868 Patent, Col. 7, ll. 57-60 (describing the relationship between the watermark, or watermark message, and key: “The number of bits in the primary key should match or exceed the number of bits in the watermark message.”). These references clearly describe the watermark message’s use, thus the term needs no construction.

- c. Another illustrative example is found at Col. 7, ll. 33-39:

unlike other forms of manipulating **digitized sample streams** to improve quality or encode known frequency ranges, an engineer seeking to provide high levels of protection of copyrights, ownership, etc. is concerned with the size of a given key, the size of **the watermark message and the most suitable area and method of insertion.**

In this example, we are instructed that the watermark message is inserted into a digitized sample stream.

- d. The invention describes “a watermarking system [that] can successfully create random keys and watermark messages that subsequently cannot be located and erased without possession of the key that acts as the map for finding each encoded watermark.” Col. 10, ll. 32-39. This description is

particularly helpful because it shows that a watermark message may be embedded and later found by a key.

- e. Although the term “watermark message” appears throughout the specification, I believe the above examples are sufficient to show that the term “watermark message” is definite. It is a term understood by one of ordinary skill in the art and is also sufficiently described in the specification.

12. '609 Patent, Claims 13 and 17, “wherein the plurality of codecs is selected based on a predefined criterion comprising one of the group consisting of: robustness, imperceptibility, security, said codec’s association with the encoding of at least one watermark, upgradability, variance of encode or decode functions, and combinations thereof”

- a. This disputed term is a collection of terms readily understood by one of ordinary skill in the art. I am not aware of whether MSI has indicated what portion of this term it finds problematic, so I will speak to the whole term. However, given the breadth of this disputed term, I reserve the right to supplement my declaration in the event MSI narrows its allegation to a particular portion.
- b. **“codec”**: One of ordinary skill in the art understands that a codec allows for the encoding and decoding of a signal. The specification even defines this term as such: “a new CODEC (encoder/decoder).” Col 20, ll. 49-50.
- c. **“robustness”**: One of ordinary skill in the art understands that a watermark may be considered robust if it is able to withstand certain

common operations that may alter the watermarked signal. The more robust a watermark, the more it is capable of withstanding alternations to the underlying signal. The patent's specification describes how "differences of robustness" may be determined because "a sample window size of 15 seconds can be compared to an implementation using a sample window size of 45 seconds." Col. 20, ll. 59-64.

- d. **"imperceptibility"**: One of ordinary skill in the art understands that it is often the goal of watermarking to make a watermark message imperceptible. The patent's specification describes how it can achieve this goal, for instance, when it describes how "the design goal of the present invention in preanalyzing a signal to mask the digital watermarks makes imperceptibility possible." Col. 15, ll. 64-66. In addition to making the watermark message imperceptible, the patent also describes that "quantization noise can be made imperceptible with perceptual coders." Col. 18, ll. 19-20.
- e. **"security"**: One of ordinary skill in the art understands that another common watermarking goal, especially in certain contexts such as copyright protection, is that of security, a term that describes how an attacker may know how an embedding algorithm operates but will still not be able to locate the watermark message without the watermark key. The specification describes how a watermark message may be made more secure: "The second method for varying of the encoding/decoding algorithms corresponds to **increased security**. . . . In this method, the

Framework selects a new CODEC, from among a list of predefined CODECs, to which to pass the sample frame as a function of the pseudo-random key employed to encode/decode the watermark” Col. 20, l. 65-Col. 21, l. 6.

- f. ***“said codec’s association with the encoding of at least one watermark”***: The individual terms here have already been addressed, and the specification describes how a codec may be associated with a watermark, for instance, how “the Framework selects a new CODEC, from among a list of predefined CODECs, to which to pass the sample frame as a function of the pseudo-random key employed to encode/decode the watermark.” Col. 21, ll. 2-6.
- g. ***“upgradability”***: One of ordinary skill in the art understands that something that is upgradable allows for being improved. The concept of upgradability is described in the ’213 Patent: “This ability can be used to provide upgrades to the watermark system, without breaking support for decoding watermarks created by previous versions of the system.” ’213 Patent, Col. 3, ll. 55-58.
- h. ***“variance of encode or decode functions”***: As already described, one of ordinary skill in the art understands that a watermark message is encoded into a digital signal and later decoded from the same signal. The patent describes how different encoding and decoding algorithms may be used. For instance, the specification discusses “the architecture to provide automated variance of algorithms to encode and decode a single

watermark.” Col. 20, 53-56. Similarly, the patent teaches “varying of the encoding/decoding algorithms corresponds to increased security.” Col. 20, ll. 65-66.

- i. I believe the above examples are sufficient to show that the term “wherein the plurality of codecs is selected based on a predefined criterion comprising one of the group consisting of: robustness, imperceptibility, security, said codec’s association with the encoding of at least one watermark, upgradability, variance of encode or decode functions, and combinations thereof” and its component parts are definite. This term is readily understood by one of ordinary skill in the art and is also sufficiently described in the specification.

13. ’213 Patent, Claims 33-40, 42, 44, “detecting and/or decoding at least one digital watermark from an encoded content signal”

- a. As described above, one of ordinary skill in the art understands that a digital watermark is encoded in a signal for later decoding.
- b. A watermark message may be detected before it is decoded, or detected and then not decoded. The specification teaches that this is “made possible for parties possessing a decoder to verify the presence of valid watermarks in a data stream, without accessing the contents of the watermark.” Col. 3, ll. 35-38.
- c. The specification also describes that it “would also be possible to scan or search archives for files containing watermarked content, and to verify

the validity of the presence of such files in an archive, by means of the information contained in the watermarks.” Col. 3., ll. 38-41.

- d. I believe the above examples show that the term “detecting and/or decoding at least one digital watermark from an encoded content signal” is definite. This term is readily understood by one of ordinary skill in the art and is also sufficiently described in the specification.

14. ’213 Patent, Claims 36 “wherein . . . selected from a group comprising: a random key; a candidate key; a pseudo-random key; a watermark key; a watermarking key; a private key; a public key; a semiprivate key; a master framework key; and, a digital watermark key.”

- a. This disputed term is a collection of terms readily understood by one of ordinary skill in the art. I am not aware of whether MSI has indicated what portion of this term it finds problematic, so I will speak to the whole term. However, given the breadth of this disputed term, I reserve the right to supplement my declaration in the event MSI narrows its allegation to a particular portion.
- b. **“a watermark key; a watermarking key; a digital watermark key”**: As described above, a watermark message may be detected and/or decoded by a key. The patent’s abstract teaches that a “watermarking key includes a binary sequence and information describing the application of that binary sequence to the content signal.”
- c. **“random key; pseudo-random key”**: The specification teaches: “Digital watermarks can be encoded with random or pseudo-random keys, which

act as secret maps for locating the watermarks. These keys make it impossible for a party without the key to find the watermark.” Col. 3, ll. 14-17. It is understood by one of ordinary skill in the art that “random” implies that the key is created by a random process, while a pseudo-random key only appears to have been created randomly.

- d. **“a private key; a public key; a semiprivate key”**: “The present invention relates to methods for the management and distribution of digital watermark keys (e.g. private, semiprivate and public) and the extension of information associated with such keys in order to create a mechanism for the securitization of multimedia titles to which the keys apply.” Col. 5, ll. 32-36. The patent’s specification provides great detail about the varying utility of these keys:

Multichannel watermarks with **private, semiprivate and public keys** used as different levels of neighboring rights assist in the creation of a self-contained model for the exchange of copyrighted works. **Private key watermarks** can be inserted into content to establish ownership rights (copyright, master right, etc.) with the content creator or an agent of the content creator maintaining control over the key. **Semiprivate watermark keys** can exist in a separate channel of the information signals that make up the work to be exchanged for subsequently delegating responsibility to distributors or sales entities to restrict resale rights in the same manner that physical goods have an exchange of title corresponding to their sale. And finally, **public watermark keys** exist as an independent component of the identification, authentication or advertising of a given work to be widely distributed over networks for initiating the purchase of a sought-after work.

Col. 5, ll. 1-16. And the patent also distinguishes these terms from their more common use in the context of encryption: “To differentiate the present invention from the art of public key cryptography, use of ‘private,’ ‘semiprivate,’ and ‘public’ keys refers only to the use of such ‘information’ with the stated purpose of distributing goods and watermarking content, not encryption or cryptography in the general sense.” Col. 5, ll. 37-41.

- e. **“*candidate key*”**: This term is readily understood by one of ordinary skill in the art. It simply implies a given key is a candidate that may be used in an attempt to encode or decode a watermark. The ’868 Patent describes how when “only a single, or limited number of watermark keys would be used to mark samples” then “the decode key candidates are limited” in this particular scenario. ’868 Patent, Col. 18, 7-14.
- f. **“*master framework key*”**: This term is described in various patents naming a common inventor with the patents-in-suit: Scott Moskowitz. *See* U.S. Patent 8,774,216, Col. 20:53 - Col. 21:10; U.S. Patent 7,830,915, Col. 20:57 - 21:17; and U.S. Patent 7,362,775, Col. 21:5-45 “According to an advantageous embodiment of the present invention, an active scheme is implemented which is described as follows. The farthest party upstream, who presumably controls the ultimate copyrights and distribution rights of the data generates two keys. The first key is a regular watermark key, as described in previous related patent application disclosures by The DICE Company, particularly, including

the “Method for Stega-Cipher Protection of Computer Code” application. This key is used for actual encoding and decoding of information from the watermark channel “owned” by this party. The second key is a new type of watermark key, called a master framework key, which dictates how the entire data stream in general is to be packetized; how the data stream packets are to be allocated among a predetermined number of reserved watermark channels; and how the channels are to be assigned to downstream parties.” [US Patent 7,770,017](#), Col. 29:45-62

- g. I believe the above examples are sufficient to show that the term “wherein . . . selected from a group comprising: a random key; a candidate key; a pseudo-random key; a watermark key; a watermarking key; a private key; a public key; a semiprivate key; a master framework key; and, a digital watermark key” and its component parts are definite. This term is readily understood by one of ordinary skill in the art and is also sufficiently described in the specification.

15. '213 Patent, Claim 42, “the key used for decoding”

- a. As I have explained above, a key may be used to decode a watermark. The patent’s specification explains: “Digital watermarks can be encoded with random or pseudo-random keys, which act as secret maps for locating the watermarks. These keys make it impossible for a party without the key to find the watermark.” Col. 3, ll. 14-17. This description

shows how a key is necessary to decode a watermark that has been encoded with random or pseudo-random keys.

- b. I believe the above example is one of many showing that the term “the key used for decoding” is definite. This term is readily understood by one of ordinary skill in the art and is also sufficiently described in the specification.

16. '213 Patent, Claim 44, “wherein the step of detecting and/or decoding . . . is separate from the encoding process”

- a. The patent’s specification describes at length that it “is also desirable to separate the functionality of the decoder side of the process to provide fuller recognition and substantiation of the protection of goods that are essentially digitized bits, while ensuring the security of the encoder and the encoded content.” Col 3, ll. 27-32. The specification describes how “[s]eparating the decoder from the encoder can limit the ability to reverse the encoding process while providing a reliable method for third parties to be able to make attempts to screen their archives for watermarked content without being able to tamper with all of the actual watermarks.” Col. 11, ll. 32-36. The patent describes that this might be accomplished

by placing separate signals in the content using the encoder, which signal the presence of a valid watermark, e.g. by providing a “public key accessible” watermark channel which contains information comprised of a digitally signed digital notary registration of the watermark in the private channel, along with a checksum verifying the content stream. The checksum reflects the unique

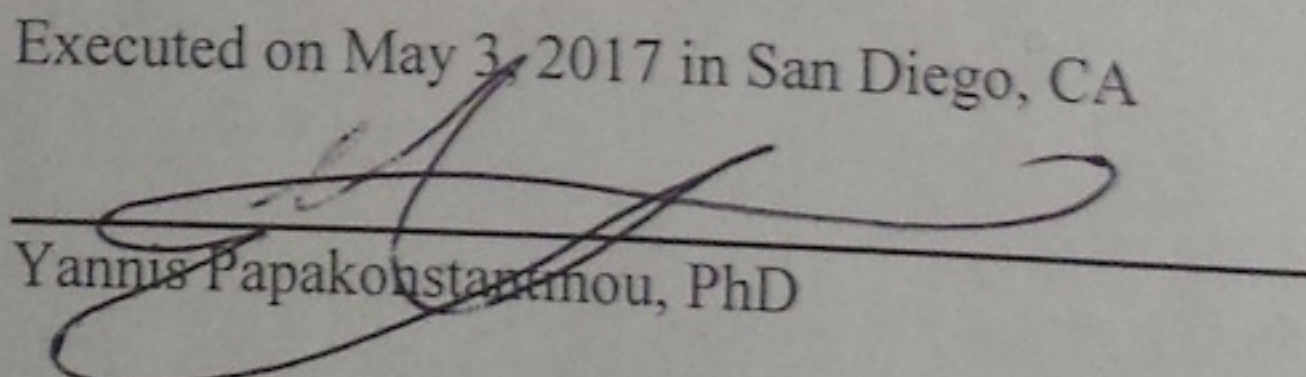
nature of the actual samples which contain the watermark in question, and therefore would provide a means to detect an attempt to graft a watermark lifted from one recording and placed into another recording in an attempt to deceive decoding software of the nature of the recording in question. During encoding, the encoder can leave room within the watermark for the checksum, and analyze the portion of the content stream which will contain the watermark in order to generate the checksum before the watermark is encoded. Once the checksum is computed, the complete watermark certificate, which now contains the checksum, is signed an/or encrypted, which prevents modification of any portion of the certificate, including the checksum, and finally encoded into the stream. Thus, if it is somehow moved at a later time, that fact can be detected by decoders.

Col. 11, ll. 36-68.

17. I believe the above example is one of many that shows that the term “wherein the step of detecting and/or decoding . . . is separate from the encoding process” is definite. This term is readily understood by one of ordinary skill in the art and is also sufficiently described in the specification.
18. In summary, as one of ordinary skill in the art, I believe that all of the terms identified by MSI are definite and sufficiently described in the patent specifications.

I declare under penalty of perjury under the laws of the United States that the statements in this declaration are true and correct.

Executed on May 3, 2017 in San Diego, CA


Yannis Papakonstantinou, PhD